Common Policy Change Proposal
Change Number: *2006-01*

To: Federal PKI Policy Authority
From: National Institute of Standards and Technology
Thru: Certificate Policy Working Group
Subject: Proposed modifications to the Common Certificate Policy
Date: 30 January 2006
Title: Alignment of Common Authentication Policies with FIPS 201

Attachment: X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, V1.2, 19 January 2006.

Version and Date of Certificate Policy Requested to be changed:
X.509 Certificate Policy for the Common Policy Framework Version 2.3,
19 September 2005.

Change Advocates Contact Information:
Name: Tim Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: tim.polk@nist.gov

Organization requesting change:
National Institute of Standards and Technology

Change summary: This change proposal resolves contradictions between FIPS 201 and the Common Policy Framework with respect to key usage, cryptographic algorithms, cryptographic migration timelines, certificate subject names, and user authentication requirements for cryptographic module activation or private key operations. FIPS 201 also mandates including of additional certificate extensions; this CP change proposal also references an updated certificate and CRL profile.

Background: These requirements are imposed by FIPS 201 and the supporting document NIST SP 800-78, in response to Homeland Security Presidential Directive 12 and agency and industry comments on the draft FIPS.

Issue

Agencies are required to issue PIV Authentication certificates as one component of their FIPS 201 implementation. The Common Policy Framework generally treats PIV authentication certificates as digital signature certificates, but FIPS 201 establishes significant differences. Clarifications to the Common Policy will simplify agency implementation of FIPS 201. NIST SP 800-78 added support for the RSA signature algorithm with PSS padding, but the Common Policy only specifies RSA signatures using the PKCS #1 v1.5 encoding.

Specific Changes:

Specific changes are made to the sections: forward, 1, 1.2, 1.3.3, 3.1.1, 3.1.3, 4.4.4, 6.1.5, 6.1.9, 6.2.1, 6.2.4.2, 6.2.7, 7.1, 7.1.3, 7.1.4, 7.1.6, 7.1.10, 9, 10, and 11. Insertions are underlined, deletions are in ~~strikethrough~~.

FOREWORD

Modify the first paragraph of the forward as follows:

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates ~~three~~ six specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, ~~and~~ a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy.

1. INTRODUCTION

Modify the second and third paragraphs of section 1 as follows:

This Certificate Policy (CP) includes ~~three~~ six distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, ~~and~~ a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all ~~three~~ six policies.

The user policies apply to certificates issued to Federal employees, contractors and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to Federal systems that have not been designated national security systems. ~~This CP implements a level of assurance comparable to or greater than the Federal Bridge Certification Authority (FBCA) Medium Assurance Policy.~~

1.2 IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain either the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. Certificates issued to devices under this policy include the id-fpki-common-devices.

Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth. ~~The id-fpki-common-authentication policy is identical to id-fpki-common-hardware, excepting the key usage constraints as mentioned in Section 7.1.10.~~

1.3.3 Applicability

Modify the third paragraph of 1.3.3 as follows:

Credentials issued under the ~~user software policy~~ id-fpki-common-policy policy are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the ~~user hardware policy~~ id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

3.1.1 Types of Names

Modify the first paragraph of 3.1.1 as follows:

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High and id-fpki-common-devices, t~~T~~he CA shall assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; ~~and~~ or an Internet domain component name.

Append the following to section 3.1.1:

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is optional. If assigned, distinguished names shall follow the rules specified above for id-fpki-common-hardware. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the

subject alternative name extension shall include the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take the following form:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], serialNumber=*FASC-N*

> Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in [USGold]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

4.4.4 Online Revocation/Status Checking Availability

CAs shall support online status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth. Status information maintained by the OCSP server must be updated regularly. Where a certificate is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours. Where a certificate is revoked for a reason other than key compromise, the status information must be updated and available to relying parties within 18 hours. CAs that do not issue certificates under id-fpki-common-authentication and relying party client software may optionally support online status checking. Because not all operational environments can accommodate online communications, all CAs will be required to support CRLs. Client software using online status checking need not obtain or process CRLs.

6.1.5 Key Sizes and Signature Algorithms

This CP requires use of RSA PKCS#1, RSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys. [Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.]

Trusted Certificates shall contain subject public keys of at least 2048 bits for RSA or 224 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA and 163 bits for elliptic curve algorithms. Certificates that expire on or after ~~January 1, 2009~~ December 31, 2010 shall be generated with at least 2048 bit keys for RSA and 224 bit keys for elliptic curve algorithms.

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-224, or SHA-256 hash algorithm when generating digital signatures. ~~RSA PKCS #1 signatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1.~~ RSA ~~PKCS #1~~ signatures on certificates and CRLs that ~~are issued on or after January 1, 2009~~ expire on or after December 31, 2010 shall be generated using SHA-256. ECDSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-224 or SHA-256, as ~~the~~ appropriate ~~hash algorithm~~ for the key length.

~~End entity certificates that expire before January 1, 2009 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates that expire on or after January 1, 2009 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.~~

End entity certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-device that expire before December 31, 2010 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-device that expire on or after December 31, 2010 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.

End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire before December 31, 2008 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire on or after December 31, 2008 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or 163 bit elliptic curve keys through 12/31/08. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or 224 bit elliptic curve keys after 12/31/08.

6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into human subscriber ~~user~~ certificates shall be used only for signing or encrypting, but not both. Subscriber certificates that assert id-fpki-common-authentication or id-fpki-common-cardAuth shall only assert the *digitalSignature* bit. Other human subscriber ~~User~~ certificates to be used for digital signatures ~~(including authentication)~~ shall assert the *digitalSignature* and~~/or~~ *nonRepudiation* bits. ~~User~~ Subscriber certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Subscriber certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits. ~~If the CA certificate is to be used to verify both certificate and CRLs, both the *keyCertSign* and *cRLSign* bits shall be asserted.~~

Public keys that are bound into device certificates may be used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates shall not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

6.2.1 Standards for Cryptographic Module

Modify the second paragraph of section 6.2.1 as follows:

CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under ~~either~~ the hardware users policy (id-fpki-common-hardware), one of the authentication policies (id-fpki-common-authentication or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High policy may not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private keys must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.7 Method of Activating Private Keys

For certificates issued under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High and id-fpki-common-devices, t~~T~~he subscriber must be authenticated to the cryptographic token before the activation of ~~any~~ the associated private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For certificates issued under id-fpki-common-cardAuth, subscriber authentication is not required to use the associated private key.

7.1 CERTIFICATE PROFILE

Certificates issued by a CA under this policy shall conform to either the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile [FPKI-PROF] or the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF].

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1}
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSA-PSS signatures. The following OID shall be used to specify the hash in an RSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(~~1~~ 2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1}
ansit163k1	{iso(1) identified-organization(3) certicom(132) curve(0) 1}
ansit163r2	{iso(1) identified-organization(3) certicom(132) curve(0) 15}
ansip224r1	{iso(1) identified-organization(3) certicom(132) curve(0) 33}
ansit233k1	{iso(1) identified-organization(3) certicom(132) curve(0) 26}
ansit233r1	{iso(1) identified-organization(3) certicom(132) curve(0) 27}
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansit283k1	{iso(1) identified-organization(3) certicom(132) curve(0) 16}
ansit283r1	{iso(1) identified-organization(3) certicom(132) curve(0) 17}

7.1.4 Name Forms

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, and id-fpki-common-device of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

~~and~~ The issuer field~~s~~ of ~~the base~~ certificate~~s~~ issued under the policies in this document shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

7.1.6 Certificate Policies Extension

Certificates issued under this CP shall assert one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

7.1.10 Key Usage Constraints for id-fpki-common-authentication

Certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth must include a critical keyusage extension, asserting only digitalSignature value.

9 BIBLIOGRAPHY

Modify the following bibliographic entries:

FIPS 186 — Digital Signature Standard (DSS), FIPS 186-2, ~~1994-05-19~~ January 27, 2000. ~~http://csrc.nist.gov/fips/fips186.pdf~~ http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FPKI-PROF — Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile. http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls http://www.cio.gov/fpkipa/documents/fpki_certificate_profile.pdf

PKCS#12 — PKCS 12 v1.0: Personal Information Exchange Syntax ~~Standard, April 1997~~ June 24, 1999 ~~Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html~~ ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

Add the following bibliographic entries:

FIPS 201 — Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201, February 25, 2005. http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

CCP-PROF — X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf

E-Auth E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003.

PACS *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004. http://smart.gov/information/TIG_SCEPACS_v2.2.pdf

PKCS#1 Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003.

RFC 2560 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999.

Delete the final paragraph in section 9:

~~Note: add [E-Auth] when issued by OMB.~~

10 ACRONYMS AND ABBREVIATIONS

Add the following acronym:

FASC-N Federal Agency Smart Credential Number
OCSP Online Certificate Status Protocol

11 GLOSSARY

Modify the following glossary entry:

Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the ~~four~~ policies and cryptographic algorithms supported.

Estimated Cost:

No cost. All requirements imposed by this change proposal are already in place through FIPS 201 and NIST SP 800-78.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Common Policy CP.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	January 5, 2006
Date Presented to FPKI PA:	January 30, 2006
Date of approval by FPKI PA:	February 8, 2006